**MAIL STOP AF**
PATENT
8033-1024

**IN THE U.S. PATENT AND TRADEMARK OFFICE**

In re application of

Shuji SHICHI Conf. 1070

Application No. 09/883,371 Group 3693

Filed June 19, 2001 Examiner Harish Dass

DATA SALE IMMEDIATE SETTLING METHOD AND PREPAID CARD

**PRE-APPEAL BRIEF REQUEST FOR REVIEW**

Assistant Commissioner for Patents January 18, 2008
P.O. Box 1450
Alexandria, VA 22313-1450
Sir:

Applicant requests a pre-appeal brief review of the final rejection in the above-identified application. No amendments are being filed with this request. A Notice of Appeal and a three month extension are filed herewith.

The review is requested for the reasons advanced on the attached sheets.

Respectfully submitted,

YOUNG & THOMPSON

Roland E. Long, Jr. Reg. No. 41,949
Attorney for the applicant
745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297
Telefax (703) 685-0573
(703) 979-4709

REL/fb

**REASONS IN SUPPORT OF REQUEST FOR REVIEW**

A pre-appeal brief review is respectfully requested because the rejections of independent claims 16 and 30 as obvious over KWAN 2003/0200179 in view of PARRILLO 5,239,583 include a clear factual error and a clear legal error, as explained below.

The present invention provides a user-supplied "next-time" password as part of each card validation and set by the user prior to accessing the card's monetary balance. A user-set password is a password set by the user and not a password set by the system.

See claim 16 step C)- sub-step iii) reciting the user entering another next-time password number and storing the user-input another next-time password in the database as the new, user-set next-time password number required for validation of the prepaid card in a next another action chain. This is not in the prior art. Also see step B) sub-step iii) which is similar.

KWAN teaches that the next-time password set by the merchant and the customer must accept the merchant-set code and later re-input the merchant-set code to validate the prepaid card.

This shortcoming in KWAN is not in dispute. Official Action page 5 acknowledges that KWAN does not disclose step B)- sub-step ii) or sub-step iii), or step C)- sub-step iii).

On pages 5-6 of the Official Action, there is a paragraph that lists "well known" actions. That these are well known now is not evidence that these actions were known to one skilled in the art at the time of the invention. It is clear error to rely on facts not supported by the record.

PARRILLO was offered as teaching the user entering a next-time password as a new, user-set next-time password number.

This is a factual error as the PARRILLO password is not a user-set password as required by the claim. The PARRILLO Abstract discloses that the user enters a PIN code in accordance with a prescribed, but variable, sequence, the sequence being different for each transaction from the previous transaction. The user inputs the PIN by entering a sequence of alphanumeric symbols in accordance with a prescribed "start" sequence of symbols for recognition as a proper 4-digit PIN for a first transaction.

PARRILLO teaches that in "the broadest aspect of the invention, the user inputs the PIN by entering a sequence of alphanumeric symbols in accordance with a prescribed 'start' sequence of symbols for recognition as a proper 4-digit PIN for a first transaction". The system, upon recognizing the correct PIN will give the user access to the account. See column 3, line 68 that expressly teaches "At the same time, the system increments at least one of the digits of the stored PIN for that account so

that, in effect, the user must enter a new PIN to access the same account on subsequent tries." See also beginning at line 12 of column 4.

From these passages, it is clear that the system is in control of setting and remembering the passwords.

What PARRILLO teaches is that each successful login by the user causes the system to increment to the next system-set password. It is this system-set password that must be entered in the PARRILLO as part of the next transaction login.

Thus, although the PARRILLO user enters a different password for each transaction, it is a system-set password and not a user-set password. Thus, the step B), sub-step iii) and step C), sub-step iii) reciting of the user entering a new, user-set next-time password number is not disclosed.

Further, claim 16 requires that the user enter this next-time password prior to sub-step iv) of requesting a current monetary balance available on the prepaid card number. In PARRILLO, the teaching is that, upon a successful login "at the same time, the system increments at least one of the digits of the stored PIN" (line 68 of column 3 and line 1 of column 4). This action does not involve the user inputting the next-time password. PARRILLO allows the transaction (including step iv) and only thereafter when the user wishes to make another transaction

is the next-time password input by the user (corresponding to step C), sub-step i).

Additionally, although PARRILLO teaches that the system increments the PIN, there is no disclosure that the system stores the new PIN (the sequence of PINs may be pre-established and incrementing moves from on PIN to a new previously stored PIN).

Further, see that step B), sub-step iii) and step C), sub-step iii) explicitly require "storing the user-input next-time password number in the database as a new, user-set next-time password number," (again prior to sub-step iv). Thus, even if a new password were stored in PARRILLO, the new password is not a user-input password as required by the claim.

Nor is there any teaching of the user-input and storing of the user-input next-time password number sub-step being performed prior to requesting a current monetary balance available on the prepaid card during a current transaction.

In this regard, PARRILLO, KWAN, and NOVOA 6,636,973 are the same in that the user does not set the password.

See in NOVOA column 3, lines 6-25 it is disclosed, beginning at line 15, (emphasis added) "At some point during or after the log on process, a biometrics account manager which has access to the users database changes the current

password associated with the use to a new password. Because the user is not required to remember and type the password, the passwords may be longer and more complex, thereby further enhancing security." If the user is not required to remember the password, it is clear that the user need not enter the new password at a later time. This passage explicitly states that the user does not type the password.

See column 3, lines 26-30 stating that the password is generated randomly. See also column 9, lines 2-9. The new password is used to log on the user; however, the user does not enter the new password. Additionally, the user does not select or enter the next-time password into the system during the current password validation.

Thus, each of these references teaches completely opposite to the recited invention where, the present invention provides that the user inputs a new next-time password after entering and verifying the current password.

Since the references do not disclose the recited features of the invention, the rejection fails based on both clear factual error and clear legal error.

Withdrawal of the rejections is therefore respectfully solicited.